Refinement of synchronizable places with multi-workflow nets : weak termination preserved!

Refinement of Synchronizable Places with Multi-workflow Nets

Weak termination preserved!

Kees M. van Hee, Natalia Sidorova, and Jan Martijn van der Werf*

Department of Mathematics and Computer Science
Technische Universiteit Eindhoven
P.O. Box 513, 5600 MB Eindhoven, The Netherlands
{ k.m.v.hee, n.sidorova, j.m.e.m.v.d.werf }@tue.nl

Abstract. Stepwise refinement is a well-known strategy in system modeling. The refinement rules should preserve essential behavioral properties, such as deadlock freedom, boundedness and weak termination. A well-known example is the refinement rule that replaces a safe place of a Petri net with a sound workflow net. In this case a token on the refined place undergoes a procedure that is modeled in detail by the refining workflow net.
We generalize this rule to component-based systems, where in the first, high-level, refinement iterations we often encounter in different components places that represent in fact the counterparts of the same procedure "simultaneously" executed by the components. The procedure involves communication between these components.
We model such a procedure as a multi-workflow net, which is actually a composition of communicating workflows. Behaviorally correct multi-workflow nets have the weak termination property. The weak termination requirement is also applied to the system being refined. We want to refine selected places in different components with a multi-workflow net in such a way that the weak termination property is preserved through refinements. We introduce the notion of synchronizable places and show that a sufficient condition for preserving weak termination is that the places to be refined are synchronizable. We give a method to decide if a given set of places is synchronizable.

1 Introduction

Complex systems are often build from components, each component having its own dedicated set of functionality. At runtime, components communicate with each other to accomplish their tasks. Every separate component can still be very complex. Therefore, an important principle in modeling component-based systems is *refinement*. In several iterations a model is refined from an abstract

* PoSecCo project (project no. 257129) is partially supported/co-funded by the European Community/ European Union/EU under the Information and Communication Technologies (ICT) theme of the 7th Framework Programme for R&D (FP7)

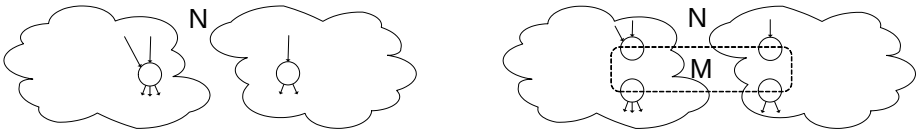


Fig. 1. Refinement of (synchronizable) places

model to a more precise model. When modeling the behavior of a system using Petri nets, one can, e.g., represent some procedure by a place in a Petri net, assuming that a token undergoes this procedure when being in this place, and later on, refine this place with the actual procedure, modelled by a workflow net.

When working with *component-based systems*, different components can contain places that together represent a single procedure. To refine the system with the actual procedure, we need to refine these places simultaneously by the procedure, as shown in Fig. 1. The same scheme can be used in the context of *Service-Oriented architectures* (SOA), where communicating services might make use of other services. The model of the procedure is then a composition of communicating workflow nets modeling the component procedures.

Consider a simple example of a procedure for booking a trip, with the system divided into three components: a travel agency, an airline and a hotel chain. The component of the agency contains place "booking a trip". In the component of the airline there is a place called "booking a seat", and in the hotel component some place "booking a room" exists. These places are related by an underlying booking procedure. In the procedure, a seat is selected at the airline, which may involve several cycles and communication with the client at the agency. Next, a reservation is made for a hotel room, which again may involve several iterations. Finally, the agency confirms the reservation at the airline. When refining the system design, we would like to refine these three places by three communicating workflow nets.

To model such a partitioned procedure, we introduce *multi-workflow nets*, being a generalization of workflow nets. Then we define the *refinement of a set of places by a multi-workflow net*, which is a generalization of the place refinement with a workflow net from [8]. A natural question that arises then is *under which conditions properties of interest are preserved through refinements.*

The property we focus on in this paper is *weak termination*, meaning that from every reachable state of a system some final state can be reached. Given a weakly terminating system with a set of places to be refined and a weakly terminating multi-workflow, we want to guarantee that the refined system is weakly terminating as well. By means of examples we motivate the requirements of "synchronizability" for the set of places to be refined, formalize this requirement and prove that if the requirement holds, *refinement of synchronizable places preserves weak termination.*

The paper is organizes as follows. In Sec. 2 we introduce basic concepts. In Sec. 3 we define the notion of multi-workflow nets and the refinement of a set of places with a multi-workflow. In Sec. 4 we give the intuition for the notion of

synchronizable places and in Sec. 5 we formalize this notion. In Sec. 6 we prove that weak termination is preserved through refinements of sets of synchronizable places. In Sec. 7 we discuss the place of our work among related works and in Sec. 8 we draw conclusions and discuss directions for future work.

2 Preliminaries

Let S be a set. The powerset of S is denoted by $\mathcal{P}(S) = \{S' \mid S' \subseteq S\}$. We use $|S|$ for the number of elements in S. Two sets U and V are *disjoint* if $U \cap V = \emptyset$. We denote the cartesian product of two sets S and T by $S \times T$. On a cartesian product we define two projection functions $\pi_1 : S \times T \to S$ and $\pi_2 : S \times T \to T$ such that $\pi_1((s,t)) = s$ and $\pi_2((s,t)) = t$ for all $(s,t) \in S \times T$. We lift the projection function to sets in the standard way, i.e. $\pi_i(U) = \{\pi_i((s,t) \mid (s,t) \in U\}$ for $U \subseteq A \times B$ and $i \in \{1,2\}$.

A *bag* m over S is a function $m : S \to \mathbb{N}$, where $\mathbb{N} = \{0, 1, \ldots\}$ denotes the set of natural numbers. We denote e.g. the bag m with an element a occurring once, b occurring three times and c occurring twice by $m = [a, b^3, c^2]$. The set of all bags over S is denoted by $\mathbb{N}^S$. Sets can be seen as a special kind of bag where all elements occur only once; we interpret sets in this way whenever we use them in operations on bags. We use $+$ and $-$ for the sum and difference of two bags, and $=, <, >, \leq, \geq$ for the comparison of two bags, which are defined in a standard way. The projection of a bag $m \in \mathbb{N}^S$ on elements of a set $U \subseteq S$, is denoted by $m_{|U}$, and is defined by $m_{|U}(u) = m(u)$ for all $u \in U$ and $m_{|U}(u) = 0$ for all $u \in S \setminus U$.

A *sequence* over S of length $n \in \mathbb{N}$ is a function $\sigma : \{1, \ldots, n\} \to S$. If $n > 0$ and $\sigma(i) = a_i$ for $i \in \{1, \ldots, n\}$, we write $\sigma = \langle a_1, \ldots, a_n \rangle$. The length of a sequence is denoted by $|\sigma|$. The sequence of length 0 is called the *empty sequence*, and is denoted by ϵ. The set of all finite sequences over S is denoted by S^*. Let $\nu, \gamma \in S^*$ be two sequences. *Concatenation*, denoted by $\sigma = \nu; \gamma$ is defined as $\sigma : \{1, \ldots, |\nu| + |\gamma|\} \to S$, such that for $1 \leq i \leq |\nu|$: $\sigma(i) = \nu(i)$, and for $|\nu| + 1 \leq i \leq |\nu| + |\gamma|$: $\sigma(i) = \gamma(i - |\nu|)$. *Projection* of a sequence $\sigma \in S^*$ on elements of a set $U \subseteq S$, denoted by $\sigma_{|U}$, is inductively defined by $\epsilon_{|U} = \epsilon$ and $(\langle a \rangle; \sigma)_{|U} = \langle a \rangle; \sigma_{|U}$ if $a \in U$ and $(\langle a \rangle; \sigma)_{|U} = \sigma_{|U}$ otherwise.

Labeled transition system A *labeled transition system* (LTS) is a 5-tuple $(S, \mathcal{A}, \longrightarrow, s_0, \Omega)$ where (1) S is a set of *states*; (2) $\mathcal{A}$ is a set of *actions*; (3) $\longrightarrow \subseteq S \times (\mathcal{A} \cup \{\tau\}) \times S$ is a *transition relation*, where $\tau \notin \mathcal{A}$ is the silent action [1]; (4) $s_0 \in S$ is the *initial state*; and (5) $\Omega \subseteq S$ is the set of *final states*.

Let $L = (S, \mathcal{A}, \longrightarrow, s_0, \Omega)$ be an LTS. For $s, s' \in S$ and $a \in \mathcal{A} \cup \{\tau\}$, we write $(L : s \xrightarrow{a} s')$ iff $(s, a, s') \in \longrightarrow$. If $(L : s \xrightarrow{a} s')$, we say that state s' is *reachable* from s by an action labeled a. A state $s \in S$ is called a *deadlock* if no action $a \in \mathcal{A} \cup \{\tau\}$ and state $s' \in S$ exist such that $(L : s \xrightarrow{a} s')$. We define $\Longrightarrow$ as the smallest relation such that $(L : s \Longrightarrow s')$ if $s = s'$ or $\exists s'' \in S : (L : s \Longrightarrow s'' \xrightarrow{\tau} s')$. As a notational convention, we may write $\xRightarrow{\tau}$ for $\Longrightarrow$. For $a \in \mathcal{A}$ we define $\xRightarrow{a}$ as the smallest relation such that $(L : s \xRightarrow{a} s')$

if $\exists s_1, s_2 \in S : (L : s \Longrightarrow s_1 \xrightarrow{a} s_2 \Longrightarrow s')$. We lift the notations of actions to sequences. For the empty sequence ϵ, we have $(L : s \xrightarrow{\epsilon} s')$ iff $(L : s \Longrightarrow s')$. A sequence $\sigma \in \mathcal{A}^*$ of length $n > 0$ is a firing sequence from $s_0, s_n \in S$, denoted by $(L : s_0 \xrightarrow{\sigma} s_n)$ if states $s_{i-1}, s_i \in S$ exist such that $(L : s_{i-1} \overset{\sigma(i)}{\Longrightarrow} s_i)$ for all $1 \leq i \leq n$. If a firing sequence σ exists such that $(L : s \xrightarrow{\sigma} s')$ we say that s' is *reachable* from s. The set of all reachable states from s are the states from the set $\mathcal{R}(L, s) = \{s' \mid \exists \sigma \in \mathcal{A}^* : (L : s \xrightarrow{\sigma} s')\}$.

The correctness notion we focus on in this paper is *weak termination*. An LTS $L = (S, \mathcal{A}, \longrightarrow, s_0, \Omega)$ is *weakly terminating* if $\Omega \cap \mathcal{R}(L, s) \neq \emptyset$ for all states $s \in \mathcal{R}(L, s_0)$, i.e. from every state reachable from the initial state some final marking can be reached.

Petri nets A *Petri net* N is a 3-tuple (P, T, F) where (1) P and T are two disjoint sets of *places* and *transitions* respectively; (2) $F \subseteq (P \times T) \cup (T \times P)$ is a *flow relation*. The elements from the set $P \cup T$ are called the *nodes* of N. Elements of F are called *arcs*. Places are depicted as circles, transitions as squares. For each element $(n_1, n_2) \in F$, an arc is drawn from n_1 to n_2. Two Petri nets $N = (P, T, F)$ and $N' = (P', T', F')$ are *disjoint* if and only if $(P \cup T) \cap (P' \cup T') = \emptyset$. Let $N = (P, T, F)$ be a Petri net. Given a node $n \in (P \cup T)$, we define its *preset* ${}^\bullet_N n = \{n' \mid (n', n) \in F\}$, and its *postset* $n^\bullet_N = \{n' \mid (n, n') \in F\}$. We lift the notation of preset and postset to sets and sequences. Given a set $U \subseteq (P \cup T)$, ${}^\bullet_N U = \bigcup_{n \in U} {}^\bullet_N n$ and $U^\bullet_N = \bigcup_{n \in U} n^\bullet_N$. The preset of a sequence $\sigma \in T^*$ is the set of all places that occur in a preset of a transition in σ, i.e., ${}^\bullet_N \sigma = \{p \mid \exists 1 \leq i \leq |\sigma| : p \in {}^\bullet_N \sigma(i)\}$. Likewise, the postset of σ is the set of all places that occur in a postset of a transition in σ, i.e., $\sigma^\bullet_N = \{p \mid \exists 1 \leq i \leq |\sigma| : p \in \sigma(i)^\bullet_N\}$. If the context is clear, we omit the N in the subscript.

Let $N = (P, T, F)$ be a Petri net. A *marking* of N is a bag $m \in \mathbb{N}^P$, where $m(p)$ denotes the number of *tokens* in place $p \in P$. If $m(p) > 0$, place $p \in P$ is called *marked* in marking m. A Petri net N with corresponding marking m is written as (N, m) and is called a *marked Petri net*. A *system* $\mathcal{S}$ is a 3-tuple $((P, T, F), m_0, \Omega)$ where $((P, T, F), m_0)$ is a marked Petri net and $\Omega \subseteq \mathbb{N}^P$ is a set of *final markings*.

The semantics of a system $\mathcal{N} = ((P, T, F), m_0, \Omega)$ is defined by an LTS $\mathcal{S}(\mathcal{N}) = (\mathbb{N}^P, T, \rightarrow, m_0, \Omega)$ where $(m, t, m') \in \longrightarrow$ iff ${}^\bullet t \leq m$ and $m' + {}^\bullet t = m + t^\bullet$ for $m, m' \in \mathbb{N}^P$ and $t \in T$. We write $(N : m \xrightarrow{t} m')$ as a shorthand notation for $(\mathcal{S}(\mathcal{N}) : m \xrightarrow{t} m')$ and $\mathcal{R}(\mathcal{N}, m)$ for $\mathcal{R}(\mathcal{S}(\mathcal{N}), m)$. We say that a place p is *safe*, if $m(p) \leq 1$ for any marking $m \in \mathcal{R}(\mathcal{N}, m_0)$. *Weak termination* of a system corresponds to weak termination of the corresponding transition system.

A *workflow net* W is a 5-tuple (P, T, F, i, f) is a Petri net such that (P, T, F) is a Petri net, $i \in P$ is the initial place and $f \in P$ is the final place such that ${}^\bullet i = f^\bullet = \emptyset$ and all nodes $(P \cup T)$ of N are on a path from i to f. We say that a workflow net is weakly terminating if the system $((P, T, F), [i], [f])$ is weakly terminating.

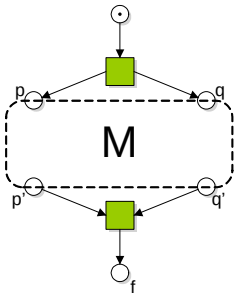
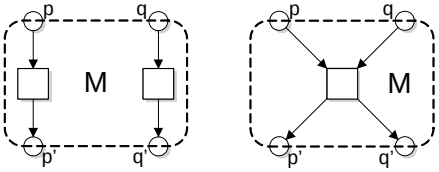


Fig. 2. Soundness skeleton for refining component



(a) Passing (b) Synchronization

Fig. 3. Simple nets to refine with

3 Refinement of Sets of Places

Many refinement/reduction rules exist for Petri nets, like the rules of Murata [13] and Berthelot [2]. Many of those rules guarantee the preservation of weak termination: applying them to a weakly terminating system results again in a weakly terminating system.

Single place refinement In [8], the authors show that a place in a workflow net may be refined with a generalized sound workflow net, while preserving the weak termination property. In this refinement, any place p can be replaced by a generalized sound workflow net (generalized soundness is weak termination of a workflow for all initial markings $[i^n], n \in I\!N$). All input arcs of p become input arcs of the initial place of the workflow net, and all output arcs of p become output arcs of the final place of the workflow net. For a safe place p, it is enough to require that both the system being refined and the refining workflow are weakly terminating, as proven in Theorem 9 from [8].

Place refinement with a weakly terminating workflow net is very useful in correctness-by-construction approaches based on stepwise refinement (see e.g. [10,14,19]).

When working with component-based information system, we often need more involved refinements: Consider e.g. a component N (modeled as a system) being an asynchronous composition of two components A and B. Suppose that place p in component A and place q in component B model at a high level counterparts of the same procedure in A and B, e.g. the payment procedure. Then p and q get refined by applying some standard workflow subcomponents C and D, possibly communicating to each other. All incoming arcs to place p are connected to the initial place of C, and all outgoing arcs from place p are connected to its final place; likewise for place q. This approach is depicted in Fig. 1; M stands there for the composition of C and D.

Multi-workflow nets To model a procedure distributed over multiple components (like net M in Fig. 1), we introduce the notion of a *multi-workflow net* (MWF net), which is a generalization of the notion used in [7]. A multi-workflow net has for each component an i/o pair consisting of an input place and an output place. Note that the definition of a MWF net with a single i/o pair coincides with the definition of a classical workflow net where the initial place is the input place and the final place the output place.

Definition 1 (Multi-workflow net). *A* multi-workflow net *(MWF net) N is a 4-tuple (P, T, F, E) where (P, T, F) is a Petri net and $E \subseteq P \times P$ is a set of* i/o pairs*, such that $|E| = |\pi_1(E)| = |\pi_2(E)|$ and ${}^\bullet\pi_1(E) = \pi_2(E)^\bullet = \emptyset$. The places in $\pi_1(E)$ are called the* input places *of N, the places in $\pi_2(E)$ are called the* output places *of N. Furthermore, each node $n \in P \cup T$ is on a path from an input place to an output place.*

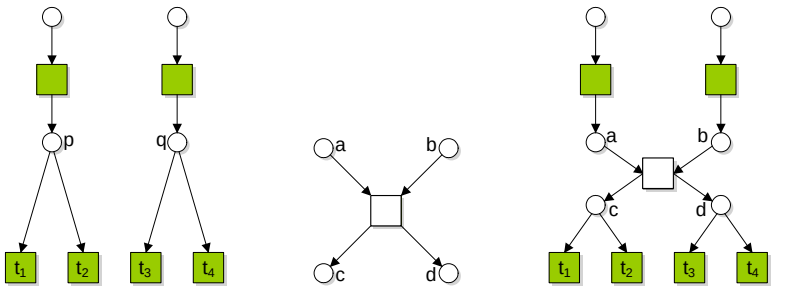
The *initial marking* of an MWF net is the marking containing one token on every input place, and the final marking is the marking containing one token on every output place. We enforce the notion of weak termination for multi-workflows with an additional requirement related to the i/o feature of multi-workflows, namely, the two places of every i/o pair should be causally connected, and thus whenever the output place gets marked the corresponding input place does not contain tokens anymore.

Definition 2 (Weak termination of an MWF net). *An MWF net $N = (P, T, F, E)$ is* weakly terminating *if (1) the system $\mathcal{N} = ((P, T, F), \pi_1(E), \{\pi_2(E)\})$ is weakly terminating and (2) $m(p) + m(q) \leq 1$ for all pairs $(p, q) \in E$ and markings $m \in \mathcal{R}(\mathcal{N}, \pi_1(E))$.*

Similar to the case of classical workflow nets (see Lemma 11 in [9]), it is easy to prove that the only marking reachable in a weakly terminating MWF net that contains the final marking is the final marking itself.

Lemma 3 (Proper completion of an MWF net). *Let $N = (P, T, F, E)$ be a weakly terminating MWF net and $m \in \mathcal{R}(\mathcal{N}, \pi_1(E))$ such that $\pi_2(E) \leq m$. Then $m = \pi_2(E)$.*

Refinement of a set of places The refinement we are interested in is the refinement of n places of a system $\mathcal{N}$ with an MWF net M. Like in place refinement, each place p belonging to the n selected places is substituted by an i/o pair: the preset of p becomes the preset of the input place of the i/o pair, the postset of p becomes the postset of the output place of the i/o pair. Fig. 4 shows an example of such a refinement. The initial marking of the refined net contains the initial marking of $\mathcal{N}$, with the tokens of the refined places being transferred to the corresponding input places of the MWF net M. Similarly, the set of final markings contains all the final markings of $\mathcal{N}$, with the tokens of the refined places being transferred to the corresponding output places of M.



(a) Net N (b) Net M (c) Refinement $N \odot M$

Fig. 4. Example of a refinement of a set of places

Fig. 5. Linear net N

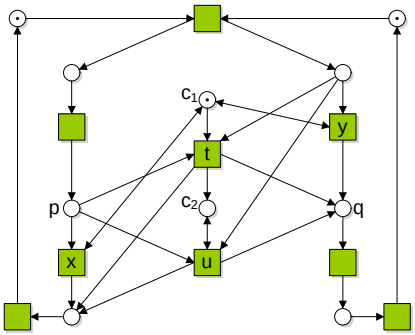
Definition 4 (Refinement of a set of places). *Let $\mathcal{N} = (N, m_{0_N}, \Omega_N)$ be a system with $N = (P_N, T_N, F_N)$ and $R \subseteq P_N$ be a set of places to be refined and $M = (P_M, T_M, F_M, E_M)$ be a MWF net, such that N and M are disjoint. Let $\alpha : R \to E_M$ be a total, bijective function. The refinement $\mathcal{N} \odot_\alpha M$ is a system $((P, T, F), m_0, \Omega)$ where*

- $P = (P_N \setminus R) \cup P_M$;
- $T = T_N \cup T_M$;
- $F = \ (\ F_N \setminus \bigcup_{r \in R}(({}_N^\bullet r \times \{r\}) \cup (\{r\} \times r_N^\bullet)) \ ) \cup F_M$
  $\quad \cup \ \bigcup_{r \in R}(({}_N^\bullet r \times \pi_1(\alpha(r))) \cup (\pi_2(\alpha(r)) \times r_N^\bullet))$;
- $m_0 = m_{0_N|P} \ + \sum_{r \in R} m_{0_N}((\pi_1 \circ \alpha)(r))$;
- $\Omega = \{m \mid \exists m_N \in \Omega_N : m = m_{N|P} \ + \sum_{r \in R} m_N((\pi_2 \circ \alpha)(r))\}$.

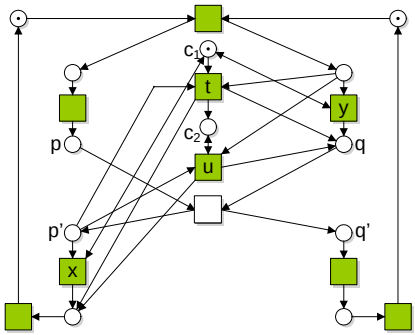
4 Intuition for the Notion of Synchronizable Places

We want to guarantee that the refinement of a set of places in a weakly terminating system by an arbitrary weakly terminating MWF net preserves weak termination. In general, this is not the case. In this section, we consider the refinement of a pair of places, in the next section we generalize the requirements to sets of places.

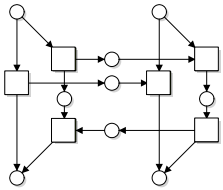
First of all, the *refined places should be safe*, i.e., in any marking reachable in the system, the place is marked with at most one token. This is needed already for the refinements of single places (see [8]). The reason lies in the definition of



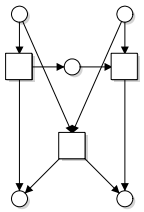
(a) Net N



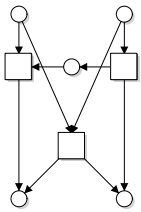
(b) Synchronizing refinement of N



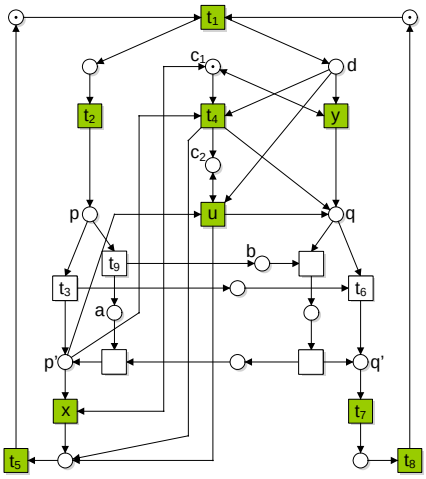
(c) MWF net M_1



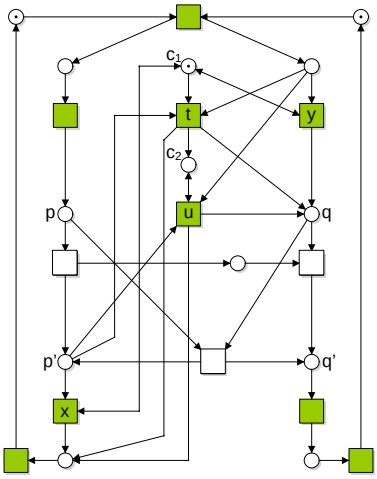
(d) MWF net M_2



(e) MWF net M_3



(f) Net $N \odot M_1$



(g) Net $N \odot M_2$

Fig. 6. Net $N \odot M_1$ is not weakly terminating while all other nets are

weak termination for MWF nets: input places contain only one token each; with more initial tokens weak termination is not guaranteed.

Another source of troubles are *causal relationships* in the refined net. Consider for example places p and q in the linear net N in Fig. 5 with initial marking $[i]$ and final marking $[f]$, which is clearly weakly terminating. The refined places p and q are causally related: the token in place p needs to be consumed before a token can be produced in place q. Refining N with the net depicted in Fig. 3(b) results in a system with a deadlock caused by the attempt to synchronize p and q. This example shows that *a reachable marking should exists in which all the places to be refined are marked to guarantee weak termination preservation.*

A first *conjecture* that it would be sufficient to check that the *synchronizing refinement of a system* (a refinement with the MWF net from Fig. 3(b)) *is weakly terminating* does not work: Consider weakly terminating system N in Fig. 6(a) with $\Omega = \{m_0, m_0 - [c_1] + [c_2]\}$, where places p and q are marked together in some reachable marking. In this net, transitions x and y are enabled as long transition t did not fire. After firing transition u, a token from place p is needed in order to mark place q.

The refinement of p and q with the net from Fig. 3(b) results in the weakly terminating net depicted in Fig. 6(b). However, the refinement of N with the weakly terminating WMF net M_1 from Fig. 6(c), depicted in Fig. 6(f), gives a deadlocking net: Indeed, firing sequence $t_1t_2t_3t_4t_5t_6t_7t_8t_1t_2t_9$ leads to marking $[a, b, c_2, d]$ being a deadlock. Note that firing $t_1t_2t_4t_5t_7t_8$ in N leads to marking $m_0 - [c_1] + [c_2]$, after the "control" token is moved from c_1 to c_2, a sort of causal relationship between p and q is introduced—they cannot be marked in the same marking of N any further. The synchronizing refinement does not show the deadlock, for the synchronizing net prevents from moving the token from c_1 to c_2.

Another attempt to find "critical" refining MWF nets is made in Fig. 6(d) and Fig. 6(e), in which the synchronizing firing and one of the two "one-way communication" options are included, thus allowing for moving the token from c_1 to c_2. Still, the refinement of N with net M_2 (Fig. 6(g)), as well as with M_3, result in a weakly terminating net, not signalling the problem exposed in $N \odot M_1$. The root of all evil is in the "AG EF" pattern of weak termination, as it would be captured in CTL [3], where AG refers to every reachable state and EF refers to the existence of a firing sequence leading to a final marking. Due to the AG-part of the requirement, the check with the synchronizing net fails—the synchronization cuts off part of the behavior. M_2 and M_3 (partially) lift the problem, but they give too much freedom for the EF part.

These examples suggest to check that N can only produce and consume tokens to/from the refined places in a certain order: a transition can only produce a "second" token in a place from the set of the refined places (with the "first" token already consumed from it) after the other refined places have been emptied. The LTS as depicted in Fig. 7 with both solid and dashed arcs describes the desired behavior for the set of two refined places. Action p (q) indicates the production of a token in place p (q), action p' (q') indicates the consumption of

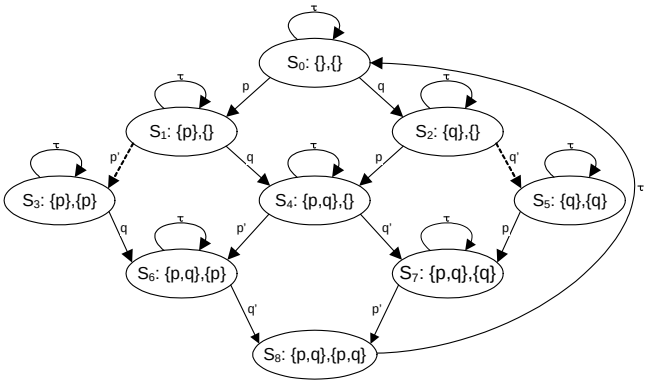


Fig. 7. May/Exit transition system for synchronizable places $\{p, q\}$

a token from place p (q). For readability reasons, each state is annotated with two sets of places: the first set indicates the places that have been marked in the current iteration, the latter indicates the places from which the token already has been consumed. The initial state is s_0.

Without loss of generality, we assume that each transition in the component performs at most one action of the LTS, implying that the refined places are "disconnected": any transition is connected once to at most one place being refined. Note that using Murata reduction rules [13] in the reverse direction, as refinements, any Petri net can be transformed to a net in which a given set of places becomes disconnected, thus this requirement does not restrict the applicability of our approach.

Definition 5 (Disconnected places). *Let $N = (P, T, F)$ be a Petri net. A set of places $R \subseteq P$ is called* disconnected *if $\forall r, s \in R : r \neq s \Rightarrow ({}^\bullet r \cup r^\bullet) \cap ({}^\bullet s \cup s^\bullet) = \emptyset$ and $\forall r \in R : {}^\bullet r \cap r^\bullet = \emptyset$.*

Now let us learn from the example in Fig. 6(a) to arrive to an idea that, as we will show later, provides a sufficient condition for weak termination preservation. To see that places p and q cannot be in the set of the refined places together, we need to observe all possible behaviour, including moving the token from c_1 to c_2, and this is supported by the LTS. The reason of the deadlock we have observed is that after reaching marking $m_0 - [c_1] + [c_2]$ we are not able to reach a marking where p and q are *both* marked. This suggests to check that from every reachable non-final state of N, some final state can be reached using only the solid transitions in Fig. 7, which is not the case for N. In the next section, we present a formalism allowing for this feature and show a sufficient condition, the principle idea of which is that for the AG-part of soundness all transitions of the LTS in Fig. 6(a) may be used, whereas for the EF-part of soundness, only the solid-line transitions can be used.

5 Formalization of Synchronizable Places

We first introduce the notion of a *may/exit transition system* with two kinds of transitions: *exit transitions*, depicted with solid lines, to model the behavior needed to guarantee termination, and *may transitions*, depicted with dashed lines, to model the behavior which is allowed but not necessary to terminate. In Fig. 7, all transitions are may transitions, and the transitions depicted with solid lines are also exit transitions. As for LTSs, we assume a set of visible actions, $\mathcal{A}$ and a silent action $\tau \notin \mathcal{A}$.

Definition 6 (May/exit labeled transition system). *A* may/exit labeled transition system (MELTS) *is a 6-tuple* $(S, \mathcal{A}, \dashrightarrow, \longrightarrow, s_0, \Omega)$ *where*

- S *is a set of* states*;*
- $\mathcal{A}$ *is a* set of actions*;*
- $\dashrightarrow \subseteq S \times (\mathcal{A} \cup \{\tau\}) \times S$ *is the set of* may transitions*;*
- $\longrightarrow \subseteq S \times (\mathcal{A} \cup \{\tau\}) \times S$ *is the set of* exit transitions*, such that* $\longrightarrow \subseteq \dashrightarrow$*;*
- $s_0 \in S$ *and* $\Omega \subseteq S$ *are the initial state and a set of final state, respectively.*

Let $L = (S, \mathcal{A}, \dashrightarrow, \longrightarrow, s_0, \Omega)$ be a MELTS. For $s, s' \in S$ and $a \in \mathcal{A} \cup \{\tau\}$, we write $(L : s \overset{a}{\dashrightarrow} s')$ when $(s, a, s') \in \dashrightarrow$, and $(L : s \xrightarrow{a} s')$ when $(s, a, s') \in \longrightarrow$. We overload the notation and write $(L : s \overset{\sigma}{\dashrightarrow} s')$ or $(L : s \xrightarrow{\sigma} s')$ for a $\sigma \in \mathcal{A}^*$ when s' can be reached (following $\dashrightarrow$ or $\longrightarrow$ respectively) from s' by some sequence $\sigma' \in (\mathcal{A} \cup \{\tau\})^*$ such that ${\sigma'}_{|\mathcal{A}} = \sigma$.

A MELTS is *properly terminating* if for every state reachable with may transitions there is a sequence of exit transitions leading to a final state.

Definition 7 (Proper termination of a MELTS). *A MELTS* $L = (S, \mathcal{A}, \dashrightarrow, \longrightarrow, s_0, \Omega)$ *is* properly terminating *if for each state* $s \in S$ *and sequence* $\sigma \in \mathcal{A}^*$ *such that* $(L : s_0 \overset{\sigma}{\dashrightarrow} s)$ *there are a sequence* $\upsilon \in \mathcal{A}^*$ *and final marking* $m_f \in \Omega$ *such that* $(L : s \xrightarrow{\upsilon} m_f)$*.*

Next, we define the MELTS as introduced in the previous section, named Sync(R). Let $\mathcal{N}$ be a system. Given a set R of disconnected places (the set of places we want to refine) in $\mathcal{N}$, we construct the MELTS Sync(R) as follows. Each state is represented by a pair of sets (I, O): set I indicates the places that have already received a token in the current iteration, and set O indicates the places from which the tokens have already been consumed in the current iteration. For each element r in R we identify two types of actions: (1) r, which adds the element r to I and (2) r', which adds the element r to O. As the places of R can be marked only once in each iteration, action r is only enabled in a state (I, O) if r is not present in I. Similarly, action r' is allowed only if $r \in I$ but $r \notin O$. For $r \in R$, action r is an exit transition, and action r' is an exit transition in a state (I, O) if I equals R; otherwise, it is a may transition. After each place of R has received and lost again a token, the state (R, R) is reached and the system returns with a silent step to the initial state, ready to another iteration. It is possible to stay at the same state performing silent actions. Fig. 7 shows the MELTS for a disconnected set of two places p and q.

Definition 8 (Sync(R)). *For a set R (of places), we define MELTS Sync(R) = $(S, \mathcal{A}, \dashrightarrow, \longrightarrow, (\emptyset,\emptyset), \{(\emptyset,\emptyset)\})$ by:*

- $\mathcal{A} = \bigcup_{r\in R}\{r, r'\}$;
- $S = \{(I,O) \mid O \subseteq I \subseteq R\}$;
- $\longrightarrow = \quad \{((I,O), r, (I',O)) \mid (I,O) \in S, r \in R \setminus I, I' = I \cup \{r\}\}$
  $\cup \quad \{((R,O), r', (R,O')) \mid (R,O) \in S, r \in R \setminus O, O' = O \cup \{r\}\}$
  $\cup \quad \{((I,O), \tau, (I,O)) \mid (I,O) \in S, I \subset R\} \cup \{((R,R), \tau, (\emptyset,\emptyset))\}$;
- $\dashrightarrow = \longrightarrow \cup \{((I,O), r', (I,O')) \mid I \subset R, r \in I \setminus O, O' = O \cup \{r\}\}$;

Corollary 9 (Proper termination of Sync(R)). *For any set R, MELTS Sync(R) as defined in Def. 8 is properly terminating.*

Each visible transition in Sync(R) corresponds to the production or consumption of a token in one of the places of R. Since we restrict our attention to sets of disconnected places, a transition either produces a token, or consumes a token from such a place. We define a mapping function h from the transitions of N to the may/exit transitions of Sync(R) that expresses this relation.

Definition 10 (Transition mapping). *Let $N = (P,T,F)$ be a Petri net, $R \subseteq P$ be a set of disconnected places and Sync(R) as defined in Def. 8. We define the function $h_{N,R} : T \to \mathcal{A}$ for every $t \in T$ by*

$$h_{N,R}(t) = \begin{cases} r & \text{if } r \in R \cap t^\bullet, \\ r' & \text{if } r \in R \cap {}^\bullet t, \\ \tau & \text{otherwise.} \end{cases}$$

We lift the notation to sequences: for a sequence $\sigma \in T^*$ of length n, $h_{N,R}(\sigma) = \langle h_{N,R}(\sigma(1)), \ldots, h_{N,R}(\sigma(n))\rangle$. If the context is clear, we omit the subscript.

We call a set R of places in a system $\mathcal{N}$ *synchronizable*, if there is a kind of refinement relation between Sync(R) and $\mathcal{N}$, namely every firing sequence of $\mathcal{N}$ can be mapped onto a may-sequence of Sync(R), covering the AG-part of weak termination; to cover the EF-part of weak termination, for every reachable marking m of $\mathcal{N}$ there should be a firing sequence leading to a final marking corresponding to some exit sequence in Sync(R). If this requirement is met, we say that the places of R are synchronizable.

Definition 11 (Synchronizable places). *Let $\mathcal{N} = (N, m_0, \Omega)$ be a system with $N = (P,T,F)$ and a set $R \subseteq P$ of disconnected places such that $m(r) = 0$ for all $r \in R$ and $m \in \Omega \cup \{m_0\}$. Let Sync$(R)$ be as defined in Def. 8. Set R is called* synchronizable *if:*

$$\forall \gamma \in T^*,\, m \in \mathcal{R}(\mathcal{N}) : (N : m_0 \xrightarrow{\gamma} m) \implies \exists s \in S, \sigma \in T^*, m_f \in \Omega :$$
$$(\mathit{Sync}(R) : (\emptyset,\emptyset) \overset{h(\gamma)}{\dashrightarrow} s) \;\wedge\; (N : m \xrightarrow{\sigma} m_f) \;\wedge (\mathit{Sync}(R) : s \xrightarrow{h(\sigma)} (\emptyset,\emptyset))$$

The definition of synchronizable places has some similarities with the notions of simulation [6] and refinement [11] and it encapsulates the definition of weak termination. In the net of Fig. 6(a) the set of places $\{p, q\}$ is not synchronizable, as after firing transition t the marking in which places p and q are both marked is not reachable.

Corollary 12 (Synchronizable places imply weak termination). *Let $\mathcal{N}$ be a system with $N = (P, T, F)$ and let $R \subseteq P$ be a synchronizable set of places. Then $\mathcal{N}$ is weakly terminating.*

Furthermore, the structure of the MELTS Sync(R) ensures that synchronizable places are safe: a firing sequence leading to a marking with more than one token on some place of R has no counterpart in Sync(R), and thus would contradict the definition of synchronizable places. By definition, synchronizable places are not marked in the initial marking nor in any final marking.

Corollary 13 (Synchronizable places are safe). *Let $\mathcal{N} = (N, m_0, \Omega)$ be a system with $N = (P, T, F)$. Let $R \subseteq P$ be a set of synchronizable places. Then each place $r \in R$ is safe.*

6 Synchronizable Places Preserve Weak Termination

In this section, we prove that weak termination is preserved through refinements of sets of synchronizable places. Given a system N with a set of synchronizable places R, and a weakly terminating MWF net M with a mapping function α, we need to prove that the refinement $\mathcal{N} \odot_\alpha M$ is weakly terminating.

By the definition of synchronizable places, every firing sequence of the system $\mathcal{N}$ can be replayed in Sync(R) using may transitions after projection. To relate reachable markings of N to the corresponding states of Sync(R), we introduce relation $Q_{N,R}$, defining it recursively, based on the firing rule of net N.

Definition 14 (Mapping markings to states). *Let $\mathcal{N} = (N, m_0, \Omega)$ be a system with $N = (P, T, F)$ and a set of disconnected places $R \subseteq P$, and Sync(R) be as defined in Def. 8. We define the relation $Q_{N,R} \subseteq \mathcal{R}(\mathcal{N}, m_0) \times S$ by:*

- $m_0 \, Q_{N,R} \, (\emptyset, \emptyset)$;
- *if $(N : m_0 \xrightarrow{\sigma} m \xrightarrow{t} m')$ for some $\sigma \in T^*$ and $t \in T$ and $m \, Q_{N,R} \, (I, O)$ then*
  - *if $\exists r \in (R \cap t^\bullet) \setminus I$ then $m' \, Q_{N,R} \, (I \cup \{r\}, O)$,*
  - *if $\exists r \in (I \cap {}^\bullet t) \setminus O$ and $O \cup \{r\} \subset R$ then $m' \, Q_{N,R} \, (I, O \cup \{r\})$,*
  - *if $\exists r \in (I \cap {}^\bullet t) \setminus O$ and $O \cup \{r\} = R$ then $m' \, Q_{N,R} \, (\emptyset, \emptyset)$*
  - *otherwise, $m' \, Q_{N,R} \, (I, O)$.*

If the context is clear, we omit the subscript.

To show that projecting an arbitrary firing sequence of the refinement $\mathcal{L}$ on the transitions of the original system $\mathcal{N}$ gives a firing sequence of $\mathcal{N}$, we first define a mapping φ of all reachable markings of $\mathcal{L}$ to markings of $\mathcal{N}$.

Definition 15 (Original net mapping). *Let $\mathcal{L} = \mathcal{N} \odot_\alpha M$ be as defined in Def. 4. We define the function $\varphi_{N,R} : T^* \to \mathbb{N}^{P_N}$ by*

$$\varphi_{N,R}(\sigma)(p) = \begin{cases} m(p), \text{ where } (N : m_{0_N} \xrightarrow{\sigma} m) & \text{if } p \in P_N \setminus R \\ m_0(p) + \sum_{t \in {}^\bullet p} |\sigma_{|\{t\}}| - \sum_{t \in p^\bullet} |\sigma_{|\{t\}}| & \text{if } p \in R \end{cases}$$

for all $\sigma \in T^*$. If the context is clear, we omit the subscript N, R.

The mapping ensures that given a firing sequence with which we reached a marking in the refined net, the mapped marking onto the original net is reachable as well, provided that the refining net is weakly terminating. If this is the case, then whenever the marking reached in $\mathcal{L}$ is mapped by φ to a marking N that is related to state $(\emptyset, \emptyset)$ in Sync(R), then the refining multi-workflow net is empty.

Lemma 16 (Trace inclusion for original net). *Let $\mathcal{L} = \mathcal{N} \odot_\alpha M$ be as defined in Def. 4 and M is weakly terminating. Let $(L : m_0 \xrightarrow{\sigma} m)$ for some $\sigma \in T^*$ and $m \in \mathcal{R}(\mathcal{L}, m_0)$. Then (1) $(N : m_{0_N} \xrightarrow{\sigma_{|T_N}} \varphi(\sigma))$ and (2) if $\varphi(\sigma)\, Q\, (\emptyset, \emptyset)$ then $m_{|P_M} = \emptyset$.*

Proof. We prove the first statement by induction on the structure of σ. Let $\sigma = \epsilon$. Then the statement holds by definition of $\odot$ and φ.

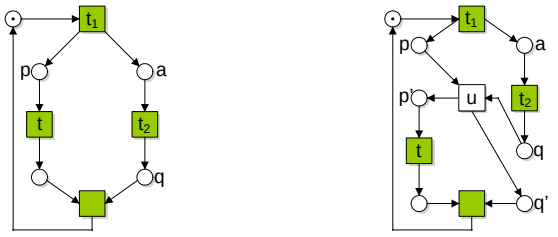
Now suppose $\sigma = \sigma'; \langle t \rangle$ for some $\sigma' \in T^*$, $t \in T$ and $m' \in \mathcal{R}(\mathcal{L}, m_0)$ such that $(L : m_0 \xrightarrow{\sigma'} m' \xrightarrow{t} m)$ and $(N : m_{0_N} \xrightarrow{\sigma'_{|T_N}} \varphi(\sigma'))$. Suppose $t \in T_M$. Then $\sigma_{|T_N} = \sigma'_{|T_N}$ and $\varphi(\sigma') = \varphi(\sigma)$. Hence, the statement holds. Next, suppose $t \in T_N$. If $R \cap {}^\bullet t = \emptyset$, then the statement directly follows from the firing rule of Petri nets and the marking equation. Otherwise, i.e., an $r \in R \cap {}^\bullet t$ exists, then by the second requirement of Def. 2, $\varphi(\sigma)(r) = 1$ since otherwise M would not be weakly terminating. Then, the statement directly follows from the firing rule of Petri nets and the marking equation.

For the second statement, we have by the synchronizability of R:

$$\exists n \in \mathbb{N} : \forall r \in R : \sum_{t \in {}^\bullet_N r} |\sigma_{|\{t\}}| = \sum_{t \in r^\bullet_N} |\sigma_{|\{t\}}| = n$$

Suppose $n = 0$. Then the statement holds by definition of $\odot$. Now suppose $n > 0$ and the statement holds for all $n' < n$. Let $r \in R$, $\sigma', \sigma'' \in T^*$, $m' \in \mathcal{R}(\mathcal{L}, m_0)$ and $\tilde{m}' \in \mathcal{R}(\mathcal{N}, m_{0_N})$ such that $\sigma = \sigma'; \sigma''$, $\tilde{m}' = \varphi(\sigma')$, $(L : m_0 \xrightarrow{\sigma'} m' \xrightarrow{\sigma''} m)$, $m'_{|P_M} = \emptyset$, $\tilde{m}'\, Q\, (\emptyset, \emptyset)$ and $\sum_{t \in {}^\bullet_N r} |\sigma''_{|\{t\}}| = 1$. Since $m'_{|P_M} = \emptyset$ and $r \in (\sigma''_{|T_N})^\bullet_N$ for all $r \in R$, we have $(M : \pi_1(E_M) \xrightarrow{\sigma''_{|T_M}} \overline{m})$ and $\pi_2(E_M) \leq \overline{m}$ for some marking $\overline{m} \in \mathcal{R}(M, \pi_1(E_M))$. By Lm. 3, $\overline{m} = \pi_2(E_M)$. Since $\varphi(\sigma)\, Q\, (\emptyset, \emptyset)$, for all $r \in R$, $r \in {}^\bullet_N \sigma''_{|T_N}$. Hence, $m_{|P_M} = \emptyset$. □

Corollary 17. *If R is a set of synchronizable places then $Q_{N,R}$ is a functional relation.*



(a) Net N (b) Net N refined with Fig. 3(b)

Fig. 8. Relation Q of Def. 15 is not a simulation relation

Note that relation Q is not a simulation relation [6]. Consider the example in Fig. 8. In this net, places p and q are synchronizable. Net N is refined with the net in Fig. 3(b). In the original net, after firing transition t_1 marking $[p, a]$ is reached and transition t is enabled. However, in the refined net, transition t cannot become enabled before transition t_2 has fired. Hence, no simulation relation exists.

We prove instead that we have the trace inclusion of the refined net into the traces of the original net when transitions of the refining net are considered as silent. A similar statement can be made for the refining MWF net M when the transitions of N are considered as silent. Here extra care should be taken in order to supply proper initial and final markings (e.g. the firing of t_1 in the refined net depicted in Fig. 8 results in marking $[p, a]$; its projection on M is $[p]$ not being reachable in M). Therefore, all places of R that have not yet been marked in the current iteration (i.e., the places of $R \setminus I$) are added to the marking of M, as well as the tokens that already have been removed from the final marking of M (i.e., the places of O).

Definition 18 (Refining net mapping). *Let $\mathcal{L} = \mathcal{N} \odot_\alpha M$ be as defined in Def. 4. We define the function $\psi_{N,R} : T^* \to \mathbb{N}^{P_M}$ by*

$$\psi_{N,R}(\sigma) = m_{|P_M} + \left(\sum_{r \in R \setminus I} \pi_1(\alpha(r)) \right) + \left(\sum_{r \in O} \pi_2(\alpha(r)) \right)$$

where $\varphi(\sigma)\, Q\, (I, O)$ and $m \in \mathcal{R}(\mathcal{L}, m_0)$ such that $(L : m_0 \xrightarrow{\sigma} m)$ for all $\sigma \in T^*$. If the context is clear, we omit the subscript N, R.

Lemma 19 (ψ maps $\mathcal{R}(\mathcal{L}, m_0)$ to $\mathcal{R}(M, \pi_1(E_M))$). *Let $\mathcal{L} = \mathcal{N} \odot_\alpha M$ be as defined in Def. 4 and M is weakly terminating. Let $(L : m_0 \xrightarrow{\sigma} m)$ for some $\sigma \in T^*$ and $m \in \mathcal{R}(\mathcal{L}, m_0)$. Then $\psi(\sigma) \in \mathcal{R}(M, \pi_1(E_M))$.*

Proof. Let $\tilde{m} = \varphi(\sigma)$ and $O \subseteq I \subseteq R$ such that $\tilde{m}\, Q\, (I, O)$. We prove the lemma by induction on the structure of σ. If $\sigma = \epsilon$, the statement holds by Lm. 16.

Now suppose $\sigma = \sigma'; \langle t \rangle$ for some $t \in T$, $\sigma' \in T^*$ and marking $m' \in \mathcal{R}(\mathcal{L}, m_0)$ such that $(L : m_0 \xrightarrow{\sigma'} m' \xrightarrow{t} m)$ and $\psi(\sigma') \in \mathcal{R}(M, \pi_1(E_M))$. Let $\tilde{m}' = \varphi(\sigma')$ and let $O' \subseteq I' \subseteq R$ such that $\tilde{m}' \, Q \, (I', O')$. Then $I' \subseteq I$ and $O' \subseteq O$. If $t \in T_M$, then ${}^\bullet t \leq {m'}_{|P_M}$, then $t^\bullet \subseteq P_M$ and the statement holds. Otherwise, assume $t \in T_N$. We need to do a case analysis based on the postset of transition t.

If $R \cap {}_N^\bullet t = R \cap t_N^\bullet = \emptyset$, then $I = I', O = O'$ and $m_{|P_M} = {m'}_{|P_M}$. Hence, the statement holds.

If $R \cap t_N^\bullet \neq \emptyset$, then a $r \in R$ exists such that $r \in t_N^\bullet$. Further, $r \notin I'$, $O = O'$ and $I = I' \cup \{r\}$, since otherwise R could not be a set of synchronizable places. By the firing rule of Petri nets, $m_{|P_M} = {m'}_{|P_M} + [\pi_1(\alpha(r))]$. In this way, we have:

$$\begin{aligned}
\psi(\sigma') &= {m'}_{|P_M} + \sum_{r \in R \setminus I'} \pi_1(\alpha(r)) + \sum_{r \in O'} \pi_2(\alpha(r)) \\
&= {m'}_{|P_M} + [\pi_1(\alpha(r))] + \sum_{r \in R \setminus I} \pi_1(\alpha(r)) + \sum_{r \in O} \pi_2(\alpha(r)) \\
&= m_{|P_M} + \sum_{r \in R \setminus I} \pi_1(\alpha(r)) + \sum_{r \in O} \pi_2(\alpha(r)) \;=\; \psi(\sigma)
\end{aligned}$$

Thus, the statement holds. A similar argument holds if $R \cap {}_N^\bullet t \neq \emptyset$.

Hence, the lemma holds. □

As a consequence of Lm. 16 and Lm. 19, boundedness is preserved by the refinement of synchronizable places.

Corollary 20 (Refinement preserves boundedness). *Let $\mathcal{L} = \mathcal{N} \odot_\alpha M$ be as defined in Def. 4 and M is weakly terminating. If $\mathcal{N}$ is k-bounded and $\mathcal{M}$ is l-bounded, then $\mathcal{L}$ is* $\max(k, l)$*-bounded.*

Lm. 19 implies that for every reachable marking m of $\mathcal{L}$ corresponding to a marking of $\mathcal{N}$ in which all synchronizable place are marked, there is a firing sequence from m in $\mathcal{L}$ using transitions of M only and leading to a marking in which all places of M are empty except for the final places. Note that in the refined net, one of the final places can already be emptied.

Corollary 21 (Completing trace of refining net). *Let $\mathcal{L} = \mathcal{N} \odot_\alpha M$ be as defined in Def. 4 and M is weakly terminating. Let $(L : m_0 \xrightarrow{\sigma} m)$ for some $\sigma \in T^*$, $m \in \mathcal{R}(\mathcal{L}, m_0)$, and let $s \in \{(R, O) \mid O \subseteq R\}$ be such that $\varphi(\sigma) \, Q \, s$. Then there are a marking $m' \in \mathbb{N}^P$ and a firing sequence $\nu \in T_M^*$ such that $(M : \psi(\sigma) \xrightarrow{\nu} f_M)$, $(L : m \xrightarrow{\nu} m')$ and ${m'}_{|P_M} \leq f_M$.*

To prove that the refinement of a set of synchronized places R preserves weak termination, we first show that for any reachable marking in the refined net that is related to the initial state of Sync(R), $(\emptyset, \emptyset)$, a firing sequence exists that reaches a final marking of the refined net.

Lemma 22 (Completing trace in refined net). *Let $\mathcal{L} = \mathcal{N} \odot_\alpha M$ as defined in Def. 4 such that M is weakly terminating. Let $\gamma \in T^*$ and $m \in \mathcal{R}(\mathcal{L}, m_0)$ such that $(L : m_0 \xrightarrow{\gamma} m)$ and $\varphi(\gamma)\, Q\, (\emptyset, \emptyset)$. Then a $\sigma \in T^*$ and an $f \in \Omega$ exist such that $(L : m \xrightarrow{\sigma} f)$.*

Proof. Let $\tilde{m}_0 = \varphi(\sigma)$. Then $\tilde{m}_0 \in \mathcal{R}(\mathcal{N}, m_{0_N})$. Since R is a set of synchronizable places, there exists a firing sequence $\mu \in T^*$ with $|\mu| = n$ and marking $f_N \in \Omega_N$ such that $(N : \tilde{m}_0 \xrightarrow{\mu} f_N)$ and $(\mathrm{Sync}(R) : (\emptyset, \emptyset) \xrightarrow{h(\mu)} (\emptyset, \emptyset))$, i.e., firing sequence μ only uses exit transitions in $\mathrm{Sync}(R)$. Since M is sound, a $\nu \in T_M^*$ exists such that $(M : \pi_1(E_M) \xrightarrow{\nu} \pi_2(E_M))$. Let $\tilde{m}_1, \ldots, \tilde{m}_n \in \mathcal{R}(\mathcal{N})$ such that $\tilde{m}_n = f_N$ and $(N : m_{i-1} \xrightarrow{\mu(i)} m_i)$ for all $1 \leq i \leq n$.

We construct sequence $\sigma = \sigma_1; \ldots; \sigma_n$ as follows:

$$\sigma_i = \begin{cases} \langle \mu(i) \rangle; \nu & \text{if } \mu(i)^\bullet \cap R \neq \emptyset \text{ and } \tilde{m}_i\, Q\, (R, \emptyset) \\ \langle \mu(i) \rangle & \text{otherwise} \end{cases}$$

Next, we need to prove that σ is a firing sequence of $\mathcal{L}$. We prove this by showing for all $1 \leq i \leq n$ the existence of markings $m_{i-1}, m_i \in \mathcal{R}(\mathcal{L}, m_0)$ such that $(L : m_{i-1} \xrightarrow{\sigma_i} m_i)$, $\varphi(\sigma_1; \ldots; \sigma_i) = \tilde{m}_i$ and if $\tilde{m}_i\, Q\, (R, O)$ for some $O \subseteq R$ then $m_{i|P_M} \leq \pi_2(E_M)$.

Suppose $n = 0$. Then $\sigma = \epsilon$. Choose $m_0 = m$. Then the statement holds trivially.

Now suppose $0 < i < n$ and a marking $m_{i-1} \in \mathcal{R}(\mathcal{L}, m_0)$ exists such that $(L : m \xrightarrow{\sigma'} m_{i-1})$ and $\varphi(\sigma') = \tilde{m}_{i-1}$ where $\sigma' = \sigma_1; \ldots \sigma\sigma_{i-1}$. Let $t = \sigma_i(1)$. Then ${}^\bullet t \leq \tilde{m}_{i-1}$, since $(N : \tilde{m}_{i-1} \xrightarrow{t} \tilde{m}_i)$. If $R \cap {}^\bullet t = \emptyset$, then $t \leq m$, and thus a $m' \in \mathbb{N}^P$ exists such that $(L : m_{i-1} \xrightarrow{t} m')$. Otherwise, an $r \in R$ exists such that $R \cap {}^\bullet t = \{r\}$. Then $\tilde{m}_{i-1}\, Q\, (R, O)$ for some $O \subseteq R$. Hence, $m_{|P_M} \leq \pi_2(E_M)$. Since ${}^\bullet t \leq \tilde{m}_{i-1}$, we have $\tilde{m}_{i-1}(r) = 1$, and hence, $m(\pi_2(\alpha(r))) = 1$. Thus, a marking $m' \in \mathbb{N}^{P_L}$ exists such that $(L : m_{i-1} \xrightarrow{t} m')$. Then $\varphi(\sigma) = \tilde{m}_i$. If $|\sigma| = 1$, choose $m_i = m'$. Then the statement holds. Otherwise, i.e., $|\sigma| > 1$, we have $\tilde{m}_i\, Q\, (R, \emptyset)$. Since $R \cap t^\bullet \neq \emptyset$, $m'_{|P_M} = \pi_1(E_M)$. Hence, a marking m_i exists such that $(L : m' \xrightarrow{\mu} m_i)$, $\varphi(\sigma) = \tilde{m}_i$ and $m_{i|P_M} = \pi_2(E_M)$. Thus, the statement holds.

Hence, σ has the desired property. □

To prove that the refinement of a set of synchronized places R preserves weak termination, we first show that from any reachable marking in the refined net, it is possible to reach a marking that corresponds to the initial state of $\mathrm{Sync}(R)$.

Now, we use the above lemma to show that from any marking reachable in $\mathcal{L}$ a final marking is reachable.

Theorem 23 (Refinement of synchronizable places preserves weak termination). *Let $\mathcal{L} = \mathcal{N} \odot_\alpha M$ be as defined in Def. 4 and M is weakly terminating. Then $\mathcal{L}$ is weakly terminating.*

Proof. Let $\gamma \in T^*$ and $m \in \mathcal{R}(\mathcal{L}, m_0)$ such that $(L : m_0 \xrightarrow{\gamma} m)$. We need to show the existence of a sequence $\sigma \in T^*$ and marking $f \in \Omega$ such that $(L : m \xrightarrow{\sigma} f)$.

Define $\tilde{m} = \varphi(\gamma)$. Then $\tilde{m}\, Q\, (I, O)$ for some $O \subseteq I \subseteq R$. Since R is a set of synchronizable places, a firing sequence $\sigma_1 \in T_N^*$ and marking $\tilde{m}_1$ exist such that $(N : \tilde{m} \xrightarrow{\sigma_1} \tilde{m}_1)$ and $(\mathrm{Sync}(R) : (I, O) \xrightarrow{h(\sigma_1)} (R, O))$, i.e., σ_1 corresponds to a firing sequence of only exit transitions in $\mathrm{Sync}(R)$.

Then $\tilde{m}_1\, Q\, (R, O)$ and $R \cap {}^\bullet\sigma_1 = \emptyset$, since otherwise $h(\sigma)$ was not a firing sequence in $\mathrm{Sync}(R)$. Then σ_1 is also a firing sequence in $\mathcal{L}$. Thus, a marking $m_1 \in I\!N^P$ exists such that $(L : m \xrightarrow{\sigma_1} m_1)$ and $\tilde{m}_1 = \varphi(\gamma; \sigma_1)$.

By Cor. 21, a firing sequence $\sigma_2 \in T_M^*$ and marking $m_2 \in I\!N^P$ exist such that $(L : m_1 \xrightarrow{\sigma_2} m_2)$, $m_{2|P_M} \leq \pi_2(E_M)$ and $\tilde{m}_1 = \varphi(\gamma; \sigma_1; \sigma_2)$.

Again since R is a set of synchronizable places, a firing sequence $\sigma_3 \in T_N^*$ and marking $\tilde{m}_2 \in I\!N^{P_N}$ exist such that $(\tilde{m}_1 : \sigma_3 \xrightarrow{\tilde{m}_2})$ and $(\mathrm{Sync}(R) : (R, O) \xrightarrow{h(\sigma_3)} (\emptyset, \emptyset))$. Since $m_{2|P_M} \leq \pi_2(E_M)$, a marking $m_3 \in I\!N^P$ exist such that $(L : m_2 \xrightarrow{\sigma_2} m_3)$ and $\tilde{m}_2 = \varphi(\gamma; \sigma_1; \sigma_2; \sigma_3)$.

By Lm. 22, a firing sequence $\sigma_4 \in T^*$ and marking $f \in \Omega$ exist such that $(L : m_3 \xrightarrow{\sigma_4} f)$. Thus, $\sigma = \sigma_1; \sigma_2; \sigma_3; \sigma_4$ has the desired property. Hence, $\mathcal{L}$ is weakly terminating. □

Clearly, synchronizability of a set of places can be effectively checked for bounded systems $\mathcal{N}$. Since weak termination can be reformulated in terms of home spaces, and the home space problem is decidable [4], we expect that the synchronizability problem is decidable for unbounded Petri nets as well.

7 Related Work

Refinements and reduction rules were in focus of the Petri nets community for a long time (see e.g. [2,13,14]). A number of rules were developed for popular subclasses of Petri nets (see e.g. [5] for reductions of free choice Petri nets, based on linear algebraic properties of these nets). The refinement we presented is a generalization of the refinement from [8] for the case of sets of places instead of a single place. In this sense our refinement is similar to the refinement $N|||_P M$ of a host net N with a daughter net M [19], but $|||_P$ is defined differently from our $\odot_\alpha$, namely, $|||_P$ basically fuses places from P in N_1 and N_2. Moreover, the focus of [19] is on the characterization of external equivalences (shown to be undecidable), while our focus is at the preservation of weak termination through refinements.

The notion of synchronizability of places is closely related to the notion of *objectivity* [15] in condition/event systems, which are Petri nets with safe places. There process semantics is used instead of interleaving semantics, and the run of a system is specified by an occurrence net, which is a, possibly infinite, acyclic marked graph. A process maps the nodes of the occurrence graph on the nodes of the condition/event system. As the net is acyclic, relation $<$ can be defined on the nodes of the net as the transitive irreflexive closure of the flow relation.

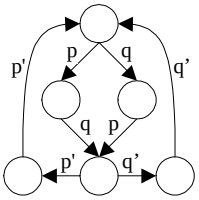


Fig. 9. LTS of places that are objective

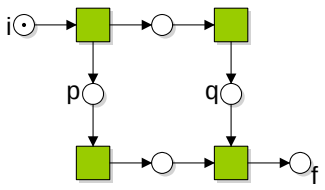


Fig. 10. Places p and q are synchronizable

Objective places need both to be marked before they can get unmarked. The notion of objectivity can be described by the LTS shown in Fig. 9. This LTS is a subgraph of the MELTS Sync (Def. 8). If two places are objective, they are also synchronizable, as the firing sequences projected on the MELTS Sync only use states s_0, s_1, s_2, s_4, s_6 and s_7. The states s_3 and s_4, i.e. the states in which place p is already unmarked but q not yet marked (or vice versa), are never reached. On the other hand, synchronizability does not imply objectivity: Consider the example of Fig. 8(a); places p and q are synchronizable, but not objective, as ${}^\bullet q \not< p^\bullet$ (since $\neg(t < t_2)$).

Note that the synchronic distance [17] between the sets of input transitions of two arbitrary places from a set of synchronizable places is at most one. This does not provide a sufficient condition for weak termination preservation through refinement, for this condition holds for input transitions of places p and q from net N in Fig. 6(a), for which a non-weakly termination refinement exists.

May/exit transition systems, which we introduce to capture the notion of synchronizability, resemble modal transition systems with may/must transitions, and the relation we establish between a Petri net and the MELTS Sync resembles the refinement relation of [11,12]. A modal transition system L refines another modal transition system L' if all the may transitions of L are also possible in L', and all must transitions of L' are also must transitions in L. The synchronizability definition resembles the necessary condition of must-soundness from [16]; there it is shown that weak termination is preserved through all possible (data) refinements iff from any configuration that is may-reachable from the start configuration, a subset of the final configurations is must-reachable. The main difference with our approach here lies in the fact that we do not require the Petri net system to have counterparts for *all* the exit transitions of the MELTS Sync, like it is done for must transitions, thus loosing the coupling as it is imposed by the refinement relation. Consider the example depicted in Fig. 10; $\{p, q\}$ is a set of synchronizable places, although the exit transition $(\text{Sync}(R) : (\emptyset, \emptyset) \xrightarrow{q} (\{q\}, \emptyset))$ can never be taken, implying that the net is not a refinement of Sync (when "exit" is renamed to "must").

An approach for checking weak termination of refinements of pairs of places is presented in [7], where the refinement is reduced to an application of synchronous composition. The check consists of two parts: one on the original net, and one on

the refining net, based on the theory of maximal controllers. We work here with *sets* of places and use a different technique in order to guarantee the preservation of weak termination for a refinement of a set of places with an *arbitrary* weakly terminating multi-workflow net.

8 Conclusions

In this paper we have defined refinements of sets of places with multi-workflows, targeted at component-based systems. We have shown that weak termination is preserved through refinements of sets of synchronizable places. We have not proven that this condition is also a necessary condition, although we have a strong belief that it is.

We plan to implement the synchronizability check for bounded Petri nets on the basis of the standard soundness check for workflow nets (see [18]), using the synchronous product of the Petri net system and the MELTS, and enforcing the EF part with the exit-path condition. We also want to find a way to compute all the maximal sets of synchronizable places for a given system and investigate how their synchronizability can be affected by other refinements.

References

1. T. Basten and W.M.P. van der Aalst. Inheritance of Behavior. *Journal of Logic and Algebraic Programming*, 47(2):47–145, 2001.
2. G. Berthelot. Transformations and decompositions of nets. In *Petri Nets, central models and their properties*, volume 254 of *Lecture Notes in Computer Science*, pages 360–376. Springer, 1987.
3. E. Clarke and E. Emerson. Design and synthesis of synchronization skeletons using branching-time temporal logic. In *Logics of Programs*, volume 131 of *Lecture Notes in Computer Science*, pages 52–71. Springer, 1982.
4. D. de Frutos Escrig and C. Johnen. Decidability of home space property. Technical report, Univ. de Paris-Sud, Centre d'Orsay, Laboratoire de Recherche en Informatique Report LRI–503, July 1989. NewsletterInfo: 35.
5. J. Desel and J. Esparza. *Free Choice Petri Nets*, volume 40 of *Cambridge Tracts in Theoretical Computer Science*. Cambridge University Press, 1995.
6. R.J. van Glabbeek. The Linear Time - Branching Time Spectrum II: The Semantics of Sequential Systems with Silent Moves. In *Proceedings of CONCUR 1993*, volume 715 of *Lecture Notes in Computer Science*, pages 66–81. Springer, 1993.
7. K.M. van Hee, A.J Mooij, N. Sidorova, and J.M.E.M. van der Werf. Soundness-preserving refinements of service compositions. In *Web Services and Formal Methods 10*, Lecture Notes in Computer Science. Springer, 2011. to appear.
8. K.M. van Hee, N. Sidorova, and M. Voorhoeve. Soundness and separability of workflow nets in the stepwise refinement approach. In *Application and Theory of Petri Nets 2003*, volume 2679 of *Lecture Notes in Computer Science*, pages 335 – 354. Springer, 2003.
9. K.M. van Hee, N. Sidorova, and M. Voorhoeve. Generalised soundness of workflow nets is decidable. In *Application and Theory of Petri Nets 2004*, volume 3099 of *Lecture Notes in Computer Science*, pages 197–216. Springer, 2004.

10. K.M. van Hee, N. Sidorova, and J.M.E.M. van der Werf. Construction of asynchronous communicating systems: Weak termination guaranteed! In *Proceedings of the 9th International Conference on Software Composition (SC 2010)*, volume 6144 of *Lecture Notes in Computer Science*, pages 106 – 121. Springer, 2010.
11. K.G. Larsen. Modal specifications. In *Automatic Verification Methods for Finite State Systems*, volume 407 of *Lecture Notes in Computer Science*, pages 232–246. Springer, 1990.
12. K.G. Larsen and B. Thomsen. A modal process logic. In *Logic in Computer Science*, pages 203–210. IEEE Computer Society, 1988.
13. T. Murata. Petri nets: Properties, analysis and applications. *Proceedings of the IEEE*, 77(4):541–580, April 1989.
14. T. Murata and I. Suzuki. A method for stepwise refinement and abstraction of Petri nets. *Journal of Computer and System Sciences*, 27(1):51 – 76, 1983.
15. W. Reisig. A strong part of concurrency. In *Advances in Petri Nets 1987*, volume 266 of *Lecture Notes in Computer Science*, pages 238–272. Springer, 1987.
16. N. Sidorova, C. Stahl, and N. Trčka. Workflow soundness revisited: Checking correctness in the presence of data while staying conceptual. In *Advanced Information Systems Engineering, 22nd Int. Conference, CAiSE 2010*, volume 6051 of *Lecture Notes in Computer Science*, pages 530–544. Springer, 2010.
17. I. Suzuki and T. Kasami. Three measures for synchronic dependence in petri nets. *Acta Informatica*, 19:325–338, 1983.
18. H.M.W. Verbeek, T. Basten, and W.M.P. van der Aalst. Diagnosing workflow processes using Woflan. *Computer Journal*, 44:246–279, 2001.
19. W. Vogler. *Modular Construction and Partial Order Semantics of Petri Nets*, volume 625 of *Lecture Notes in Computer Science*. Springer, 1992.